



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/696,518	10/25/2000	Olivier Daude	FR9-1999-0110 US1	2590
7590	04/07/2004		EXAMINER	
BRACEWELL & PATTERSON, L.L.P. INTELLECTUAL PROPERTY LAW P.O. BOX 969 AUSTIN, TX 78767-0969			QUINONES, EDEL H	
			ART UNIT	PAPER NUMBER
			2131	6
DATE MAILED: 04/07/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/696,518	DAUDE ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Edel H Quinones	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 25 October 2000.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-39 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-39 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1.) Certified copies of the priority documents have been received.  
 2.) Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3.) Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1)  Notice of References Cited (PTO-892)  
 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3)  Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
     Paper No(s)/Mail Date \_\_\_\_\_
- 4)  Interview Summary (PTO-413)  
     Paper No(s)/Mail Date. \_\_\_\_\_  
 5)  Notice of Informal Patent Application (PTO-152)  
 6)  Other: \_\_\_\_\_

***III. Detailed Action***

1. Claims 1-39 are presented for examination.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-4, 7-10, 13-17, 20-24, 27-30, 33-36 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasserman et al. (U.S. Patent 6,304,969 and Wasserman hereinafter) in view of Kaffine et al. (U.S. Patent 6,654,914 and Kaffine hereinafter) in further view of Lim et al. (U.S. Patent 5,884,024 and Lim hereinafter).

In regards to claim 1, 14 and 27, Wasserman teaches a system for preventing unauthorized servers from responding to client configuration requests (i.e. a system and method for verifying the authorization of a server to provide network resources to a client. The system can be configured to prevent software operating on the client from enabling the functions of the client without proper server authorization.) (col. 2, lines 34-47), said system comprising means for:

detecting at least one unauthorized server within said network (col. 3, lines 21-35).

Wasserman does not teach the steps of:

simulating a plurality of network clients within a server checker client; and

delivering configuration requests from said server checker client to said at least one unauthorized server such that said at least one unauthorized server is unable to respond to configuration requests from actual network clients.

Kaffine discloses a system for isolating faults in a network (col. 1, lines 5-7).

Kaffine teaches the step of simulating a plurality of network clients (i.e. users) within a server checker client (i.e. it teaches that the user and/or the network can be simulated to each other) (col. 4, lines 16-17).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman with the teachings of Kaffine to include the step of simulating a plurality of network client (i.e. users) within a server checker client with the motivation to improve the network uptime, reliability, performance and response/repair time (Kaffine, col. 4, lines 29-31).

Lim discloses a method and apparatus for reducing the probability of IP address misuse among the clients of a DHCP server (col. 1, lines 48-51).

Lim teaches that an authorized/unauthorized DHCP server can be made unable to respond to requests from network clients by repeatedly obtaining IP leases from the DHCP server (col. 2, lines 28-34). In other words, Lim teaches the step of delivering configuration requests from a server checker client to an unauthorized server such that the unauthorized server is unable to respond to configuration requests from actual network clients.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine with the teachings of Lim to include the step of delivering configuration requests from a server checker client to an

Art Unit: 2131

unauthorized server such that the unauthorized server is unable to respond to configuration requests from actual network clients with the motivation to degrade the performance of the unauthorized server (Lim, col. 2, lines 32-34).

In regards to claim 2, 15 and 28, Lim teaches reserving multiple IP addresses (i.e. exhausting the supply of IP addresses) (col. 2, lines 29-30) in each of said at least one unauthorized dynamic host configuration server.

In regards to claims 3, 16 and 29, Lim teaches that reserving multiple IP addresses in each of said at least one unauthorized dynamic host configuration server further comprises delivering a plurality of different IP address requests (i.e. IP leases) (col. 2, line 30) to each of said at least one unauthorized dynamic host configuration server.

In regards to claims 4, 17 and 30, Lim teaches the system of claims 3, 16 and 29, further comprising flooding (i.e. “IP address hogging”) (col. 2, line 28) each of said at least one unauthorized dynamic host configuration server with a plurality of IP address renewal requests (i.e. IP leases) (col. 2, lines 28-34).

In regards to claims 7, 20 and 33, Lim teaches wherein each IP address renewal request includes an unknown client IP address (col. 8, lines 16-19).

In regards to claims 8, 21 and 34, the combination of Wasserman, Kaffine and Lim teaches wherein detecting an unauthorized server comprises:

delivering a request (i.e. client message) from the client(s) by:

broadcasting a request to servers over said network (i.e. transmitting client message to server) (figure 8, step 150); and

receiving one or more responses from one or more of said servers (figure 10, step 168).

Wasserman does not teach:

identifying a specific server that originated each of said responses; and

determining for each identified server whether or not said identified server is authorized by referring to a table, wherein said table includes a list of authorized servers.

However, Wasserman teaches identifying a specific client that originated a message and determining for each identified client whether or not said identified client is authorized by referring to a table (i.e. client authorization database), wherein said table includes a list of authorized clients (i.e. registered clients) (col. 10, lines 41-62).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine and Lim with the teachings of Wasserman to include identifying a specific server that originated a response; and determining for each identified server whether or not said identified server is authorized by referring to a table, wherein said table includes a list of authorized servers with the motivation to verify the validity of the server messages (Wasserman, col. 10, lines 59-62).

In regards to claims 9, 22 and 35, the combination of Wasserman, Kaffine and Lim does not teach wherein identifying a specific server that originated a response further comprises retrieving from each response an IP address of the server that originated the response.

However, Wasserman teaches that identifying a specific client that originated a response comprises retrieving from each response an identifier of the client that originated the response (col. 10, lines 55-62). This client identifier is analogous to a client IP address.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine and Lim with the teachings of Wasserman to include wherein identifying a specific server that originated a response further comprises retrieving from each response an IP address of the server that originated the response with the motivation to verify the validity of the server messages (Wasserman, col. 10, lines 59-62).

In regards to claims 10, 21 and 36, the combination of Wasserman, Kaffine and Lim does not teach wherein said table includes an IP address for each authorized dynamic host configuration server.

However, Wasserman teaches wherein said table (i.e. client authorization database) includes a client identifier for each authorized client. This client identifier is analogous to a client IP address.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine and Lim with the teachings of Wasserman to include wherein said table includes an IP address for each authorized

dynamic host configuration server with the motivation to verify the validity of the server messages (Wasserman, col. 10, lines 59-62).

In regards to claims 13, 26 and 39, Wasserman teaches wherein detecting at least one unauthorized server is performed at predefined time intervals (i.e. when a security counter, or timer, exceeds the value of an expiration count) (col. 2, lines 48-50).

3. Claims 5-6, 18-19 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasserman in view of Kaffine in view of Lim as applied to claims 4, 17 and 30 as discussed above, in further view of Chen et al. (U.S. Patent 5,812,780 and Chen hereinafter).

In regards to claims 5, 18 and 31, the combination of Wasserman, Kaffine and Lim teaches the system of claims 4, 17 and 30 as discussed above.

The combination of Wasserman, Kaffine and Lim does not teach wherein the step of flooding each of said at least one unauthorized dynamic host configuration server with a plurality of IP address renewal requests comprises the steps of:

simulating a plurality of clients requesting renewal of their IP address; and  
delivering a plurality of different IP address renewal requests from said simulated plurality of clients to each of said at least one unauthorized dynamic host configuration server.

Chen discloses an invention relating to computer simulation systems and software testing models (col. 1, lines 8-9).

Chen teaches flooding a server with a plurality of requests by simulating a plurality of clients and delivering a plurality of requests from said simulated plurality of clients to said server (col. 15, lines 19-34).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman, Kaffine and Lim with the teachings of Chen to include that the step of flooding each of said at least one unauthorized dynamic host configuration server with a plurality of IP address renewal requests comprises the steps of simulating a plurality of clients requesting renewal of their IP address; and delivering a plurality of different IP address renewal requests from said simulated plurality of clients to each of said at least one unauthorized dynamic host configuration servers with the motivation to provide realistic load conditions on a server (Chen, col. 1, lines 13-15).

In regards to claims 6, 19 and 32, Lim teaches including within each IP address request an unknown (i.e. nonexistent or otherwise invalid) (col. 8, lines 18-19) client medium access control (MAC) address (col. 6, lines 38-44); and an IP address (i.e. trusted identifier) (col. 6, lines 2-11) of the server checker client.

4. Claims 11-12, 24-25 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasserman in view of Kaffine in view of Lim et al as applied to claims 8, 21 and 34 above, in further view of Mouko et al. (U.S. Patent 6,678,732 and Mouko hereinafter).

In regards to claims 11, 24 and 37, the combination of Wasserman, Kaffine and Lim teaches the system of claims 8, 21 and 34 as discussed above.

The combination of Wasserman, Kaffine and Lim does not teach that each response comprises a proposed IP address, and that determining for each identified server whether or not the identified server is authorized by referring to a table, further comprises releasing a proposed IP address to each server.

Mouko discloses a system that dynamically allocates IP addresses to client devices (col. 1, lines 10-11).

Mouko teaches that each response from a server comprises a proposed IP address (col. 2, lines 46-51). Mouko also teaches releasing a proposed IP address to each server after utilizing the information contained in the message (i.e. determining for each identified server whether or not the identified server is authorized) (col. 7, lines 25-27)

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine and Lim with the teachings of Mouko to include that each response comprises a proposed IP address, and that determining for each identified server whether or not the identified server is authorized by referring to a table, further comprises releasing a proposed IP address to each server with the motivation to dynamically allocate IP addresses (Mouko, col. 1, line 10).

In regards to claims 12, 25 and 38, the combination of Wasserman, Kaffine and Lim teaches the system of claims 8, 21 and 34 as discussed above.

The combination of Wasserman, Kaffine and Lim does not teach that releasing the IP address further comprises broadcasting a release message containing an IP address of an unknown server to each of the identified servers.

Mouko teaches that a server A leases an IP address in response to a DHCPREQUEST message containing its server id (col. 4, lines 8-14). Conversely, if the DHCPREQUEST message sent by the client contains the server id of any other client (including an unknown server), server A releases the IP address. Therefore, Mouko teaches that releasing the IP address further can be accomplished by broadcasting a release message containing an IP address of an unknown server to each of the identified servers

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Wasserman and Kaffine and Lim with the teachings of Mouko to include that releasing the IP address further comprises broadcasting a release message containing an IP address of an unknown server to each of the identified servers with the motivation to dynamically allocate IP addresses (Mouko, col. 1, line 10).

*Other Prior Art Made of Record*

5.     A.     Massarani (U.S. Patent No. 6,393,484) discloses a system and method for controlled access to shared-medium public and semi-public internet protocol (IP) networks;
- B.     Sawyer et al. (U.S. Patent No. 6,466,986) discloses a method and apparatus for providing dynamic host configuration protocol (DHCP) tagging; and
- C.     Beser (U.S. Patent No. 6,189,102) discloses a method for authentication of network devices in a data-over cable system.

Art Unit: 2131

***Conclusion***

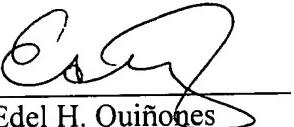
6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

***Points of Contact***

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H. Quiñones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.



Edel H. Quiñones  
Patent Examiner  
Technology Center 2100

March 31, 2004



AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100